



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/051,249	01/22/2002	Olli Immonen	4208-4034US2	8865

27123 7590 09/07/2005
MORGAN & FINNEGAN, L.L.P.
3 WORLD FINANCIAL CENTER
NEW YORK, NY 10281-2101

EXAMINER

SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 09/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/051,249

Applicant(s)

IMMONEN ET AL.

Examiner

Michael J. Simitoski

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 21 November 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-58 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 35-42 and 51-58 is/are allowed.
- 6) ☒ Claim(s) 1-30, 33, 34, 43-46, 49 and 50 is/are rejected.
- 7) ☐ Claim(s) 31, 32, 47 and 48 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 June 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 1/22/02, 6/3/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☒ Other: See Continuation Sheet.

Continuation of Attachment(s) 6). Other: IDS of 3/6/2003, 5/3/2005 & 6/24/2005 .

DETAILED ACTION

1. The IDS of 1/22/2002, 6/3/2002, 3/6/2003, 5/3/2005 & 6/24/2005 were received and considered.
2. Claims 1-58 are pending.

Claim Objections

3. Claim 38 is objected to because of the following informalities:

Regarding claim 38, “consisting the” (end of line 2) should be replaced with “consisting of”;

Regarding claim 51, “current value of counter” should be replaced with “current value of the counter”;

Regarding claim 56, “of the” (line 2) is recited twice;

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 29, 32-34, 43 & 49-50 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. All claims are interpreted as best understood.

Regarding claim 29, it is unclear as to which certificate each of: “the certificate” (line 4), “said certificate” (line 5) and “received certificate” (line 6) is referring.

Regarding claim 32, it is unclear as to if “the third party” (lines 2, 4-6, 8 & 10) is referring to “the third party device”; for the purposes of this Office Action, it is assumed to refer to “the third party device”.

Regarding claim 33, there is no antecedent basis for the limitation “the received counter ID” (lines 3-4).

Regarding claim 33, there is no antecedent basis for the limitation “said third party public key” (line 4).

Regarding claim 34, there is no antecedent basis for the limitation “the received counter ID” (line 4).

Regarding claim 34, there is no antecedent basis for the limitation “said third party public key” (line 4).

Regarding claim 43, there is no antecedent basis for the limitation “the security element” (line 3).

Regarding claim 49, there is no antecedent basis for the limitation “the received counter ID” (lines 3-4).

Regarding claim 49, there is no antecedent basis for the limitation “received public key” (line 4).

Regarding claim 50, there is no antecedent basis for the limitation “the received counter ID” (lines 3-4).

Regarding claim 50, there is no antecedent basis for the limitation “received public key” (line 4).

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claim 1-2, 4-6, 9, 13, 15-21, 24-28, 30, 43-44 & 46 rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication 2002/0094090 to Iino.

Regarding claims 1-2, 4-6, 9, 15-21, 25-27, 30 & 46, Iino discloses a mobile equipment/ticket storage device including a first storage device/storage unit (Fig. 7, #28), a security element/ticket storage device that includes a second storage device (Fig. 7, #28), at least one third-party device/ticket issuing device (Fig. 1) and a processor/ticket assignment controller (Fig. 7, #21) in communication with said first storage device/storage unit, said second storage device/storage unit and said third-party device/ticket checking device (Figs. 1 & 7) configured to authenticate the security element/ticket storage device (¶12, 324 & Fig. 14), create and initiate at least one counter (¶103-104, ¶154, ¶282 & ¶302-304) stored in said second storage device (Fig. 7, #28) in said secure element/ticket storage device (¶81, ¶103-110), receive at least one electronic ticket from said third-party device/ticket issuing device and storing said at least one electronic ticket in the first storage device/storage unit (Fig. 12) and redeem said at least one electronic ticket stored in said first storage device/storage unit with said at least one third-party device/ticket checking device (Fig. 18 & ¶80).

Regarding claims 13, 28 & 43-44, Iino discloses a system as described above, further disclosing a certificate (Fig. 4) and a pair of encryption keys (Fig. 4) and that the third-party device/ticket issuing device has a cryptographic master public key (Fig. 2) and is configured to issue tickets (¶78).

Regarding claim 24, Iino discloses storing a master key/secret key in a third-party device (Figs. 2-3).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Iino, as applied to claim 1 above, in further view of U.S. Patent 6,690,794 to Terao et al. (**Terao**). Iino lacks explicitly a monotonically decreasing counter comprising a unique identifier and an associated current value corresponding to each of the stored electronic tickets. However, Terao teaches that a ticket is useful where both a ticket prover (holder) and verifier mutually authenticate using public key authentication, which causes the decrementing of a counter (col. 30, line 60 – col. 33, line 18) for use in prepaid card systems. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a counter that is monotonically decrementing. One of ordinary skill in the art would have been motivated to perform such a

Art Unit: 2134

modification for use in prepaid card systems, as taught by Terao (col. 30, line 60 – col. 33, line 18).

10. Claims 7-8, 10-11 & 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Iino**.

Regarding claims 7-8, Iino lacks explicitly a removable memory. However, the examiner takes Official Notice that SIM cards are old and well established in the art of cellular phones and PDAs as a method of transferring data/settings from one device to another. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the tickets, etc. on a SIM module of a cell phone. One of ordinary skill in the art would have been motivated to perform such a modification to allow for the transfer of the tickets from one device to another. This advantage is well known to those skilled in the art.

Regarding claims 10-11, Iino lacks explicitly an operating system. However, the examiner takes Official Notice that operating systems are old and well established in the art of devices as a means to control the operation of the device. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was modify Iino to include an operating system on the portable storage device. One of ordinary skill in the art would have been motivated to perform such a modification to maintain predictable control over the device. This advantage is well known to those skilled in the art.

Regarding claim 22, Iino lacks explicitly a tamper-resistant removable memory. However, the examiner takes Official Notice that SIM cards are old and well established in the art of cellular phones and PDAs as a method of transferring data/settings from one device to

Art Unit: 2134

another. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the tickets, etc. on a SIM module of a cell phone. One of ordinary skill in the art would have been motivated to perform such a modification to allow for the transfer of the tickets from one device to another. Further, the examiner takes Official Notice that tamper-resistant memories are old and well established in the art of secure devices as a method of making difficult the physical disassembling of a device, which would otherwise allow reading of the data by an unauthorized user. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to design the removable memory device to be tamper-resistant. One of ordinary skill in the art would have been motivated to perform such a modification to prevent the reading of data on the memory device using external physical means. These advantages are well known to those skilled in the art.

11. Claims 12 & 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Iino**, as applied to claim 1 above, in view of "Cryptography Terminology" by **EFA**. Iino lacks the third party device comprising an encryption key pair and a signature key pair. However, EFA teaches that recommended practice when using digital signatures is to use separate key pairs for encryption and digital signatures (p. 1, §Digital Signature). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store an encryption key pair and a signature key pair in the third party device. One of ordinary skill in the art would have been motivated to perform such a modification to following recommended practice by using separate key pairs for encryption and signature processing, as taught by EFA (p. 1, §Digital Signature).

12. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Iino**, as applied to claim 18 above, in view of Handbook of Applied Cryptography by Menezes et al. (**Menezes**). **Iino** lacks explicitly the third party device storing a public key of the security element. However, Menezes teaches that it is known to store the public key of device (widely available) so as to encrypt messages to be read by only that device (§8.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store a public key of the security element in the third party device. One of ordinary skill in the art would have been motivated to perform such a modification to communicate messages to be read only by the security element, as taught by Menezes (§8.1).

13. Claims 29 & 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Iino**, as applied to claims 28 & 44 above, in view of U.S. Patent 6,816,707 to Barker et al. (**Barker**) in view of Handbook of Applied Cryptography by Menezes et al. (**Menezes**). **Iino** lacks requesting a certificate and verifying the certificate, as recited in the claims. However, Barker discloses that performing authentication between devices with their own certificates ensures against misuse (col. 3, lines 5-25). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to perform authentication between two devices each with their own certificates. One of ordinary skill in the art would have been motivated to perform such a modification to protect against misuse of the system, as taught by Barker (col. 3, lines 5-25). As modified, **Iino** is silent regarding the steps of requesting a certificate, sending the certificate, receiving the certificate and verifying the certificate. However, Menezes teaches that

Art Unit: 2134

the process for authentication using certificates instructs user B to acquire a certificate from user B, and to verify the certificate (p. 39, §1.11.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send a request to the security element for its certificate of authenticity, send a response including the certificate, receiving the certificate in the mobile equipment and verifying the certificate in the mobile equipment. One of ordinary skill in the art would have been motivated to perform such a modification to verify the authenticity of the components using certificates, as taught by Menezes (p. 39).

Allowable Subject Matter

14. Claims 35-42 & 51-58 are allowed.

15. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 35 and 42, the prior art relied upon fails to teach or suggest a counter having a message authentication key, where the security element generates an authorization token being a message authentication code computer by using the message authentication key stored in the counter, in combination with the other elements of the claim.

Regarding claims 51 & 58, the prior art relied upon fails to teach or suggest the security element generating an authorization token being a signature on authenticator data comprising the said counter ID, current value of the counter, and the public key of the security element, in combination with the other elements of the claim.

16. Claims 31 & 47-48 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Regarding claims 31 & 47, the prior art relied upon fails to teach or suggest sending from the mobile equipment to the third party device a newly created counter ID received from the security element, in combination with the other elements of the claim.

Regarding claim 48, the prior art relied upon fails to teach or suggest the third party creating at least one ticket by forming a signature on authenticator data consisting of the received counter ID, said public key of the third party, a number representing the number of allowed uses for the ticket and additional information, in combination with the other elements of the claim.

17. Claim 32 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims. Regarding claim 32, the prior art relied upon fails to teach or suggest the third party creating at least one ticket by forming a signature on authenticator data consisting of the received counter ID, said public key of the third party, a number representing the number of allowed uses for the ticket and additional information, in combination with the other elements of the claim.

Conclusion

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841.

Art Unit: 2134

The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Or faxed to:


(571) 273-8300
(for formal communications intended for entry)

Or:

(571) 273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


MJS
August 29, 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100